Manageable Fast Handover at Access Point in WLAN

Gao Yin
Li Jie
(Mobile Division of ZTE Corporation, Shanghai 201203, China)

Abstract:
The handover speed is always vital for the further development of Wireless Local Area Network (WLAN), which is enjoying a fast growth. Based on the handover technology specified in IEEE 802.11 WLAN, Manageable Fast Handover (MFHO) mechanism is proposed to speed up handover at the Access Point (AP), meet handover demands of services with different Quality of Service (QoS), and ensure service continuity. Adopting a handover policy named "Make-before-break", this mechanism enables wireless APs to control and manage handover between two stations based on improving Inter-Access Point Protocol (IAPP). Tests have been carried out to compare functions and performance of MFHO and IAPP-based handover technology. The test results prove that MFHO provides a higher successful handover ratio and better handover performance than IAPP-based handover technology.

There are increasing demands for mobility, which is the capability to move or roam, in recent years. Wireless Local Area Networks (WLAN), which combine computer networks with wireless communication technologies, are wireless networks built in local areas and support free mobility. A WLAN employs wireless multi-access channels as its transmission media, and provides the functions of a traditional wired local area network. Its users can freely enjoy the broadband network access anytime and anywhere.

Using electromagnetic waves to send and receive data in the air, the WLAN within its perimeter provides all computers with mobility. Therefore, it is a fast and easy solution to network channel connection, which is a difficult problem in cable networks. The IEEE WLAN working group studies global standards for wireless devices and networks that work at the open frequency band of 2.4 GHz with the rates at 1 Mb/s and 2 Mb/s. The group released IEEE 802.11 specifications, one of the first generation WLAN standards, in June 1997. The physical layer of 802.11 defines the signal characteristics and modulation modes of data transmission, while the Media Access Control (MAC) layer covers such technical specifications as the air interface communication protocols, including the contents for handover. The IEEE 802.11 a/b/g specifications were then released in succession to get wider data communication bandwidth and more functions, and to promote the rapid development of WLAN. The improvement of mobile performance of WLAN is certainly the key factor of its fast widespread.

Based on the study of the existing WLAN handover technology, Station (STA) initiating handover, this article proposes Manageable Fast Handover (MFHO) mechanism to ensure the efficiency and security of handover. It can be implemented by handover indication or handover request. The two handover methods all support handover based on Access Point (AP)/ Access Control (AC).

1 Manageable Fast Handover at Access Point

1.1 Popular Handover Technology for WLAN

Most existing WLAN systems follow IEEE 802.11 specifications[1] and adopt the STA initiating handover technology defined by IEEE 802.11. This technology enables an STA, according to the quality of signals at the air interface, to select the AP with the strongest signal in an Extended Service Set (ESS) as the target access point for handover, as shown in Figure 1.

According to the Inter-Access Point Protocol (IAPP), STA handover between different APs in the same ESS follows four steps[2]:

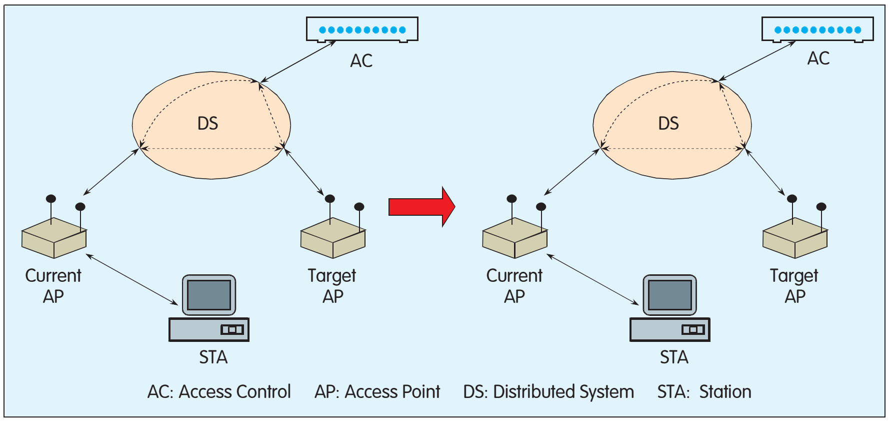
(1) The STA finds the new target AP, breaks the connection with the current AP, and sends a reconnection request to the target AP.

(2) The target AP establishes a new connection with the STA, and then sends a handover notification to the current AP while updates the Layer 2 route.

(3) When the current AP receives the notification, it will transfer the STA related information to the target AP through the security channel of Distributed System (DS), and clear the local STA related information.

(4) The target AP stores the received STA related information, and the STA switches to the target AP.

The handover, mentioned, is implemented by connection or reconnection (pre-authentication), which causes a long time delay. Therefore, services sensitive to time delay will be interrupted during handover. Furthermore, the STA handover lacks security protection, because there is no necessary security authentication for the target AP when using reconnection for handover. In addition, casual STA initiating



▲Figure 1. Process of station initiating handover.

handover will bring some difficulties to the optimization processes such as load balancing. Since the AP cannot effectively control and manage STA handover, it is hard to guarantee handover efficiency, Quality of Service (QoS), security, and optimization.

1.2 Manageable Fast Handover

This article proposes the MFHO mechanism to overcome the disadvantage of the currently used STA initiating handover technology. The MFHO puts handover control at the AP or AC, and uses the security channel of wired networks to transfer user information, including user ID, security information and service request, to the target AP, which ensures the efficiency and security of handover. It can also meet the handover requirements of services with different QoS and contributes to future expansion of multiple services. With MFHO, the process of an STA handover between different APs in the same ESS is:

(1) The STA sends information of the environment of radio air interface (or handover request) to the AP/AC.

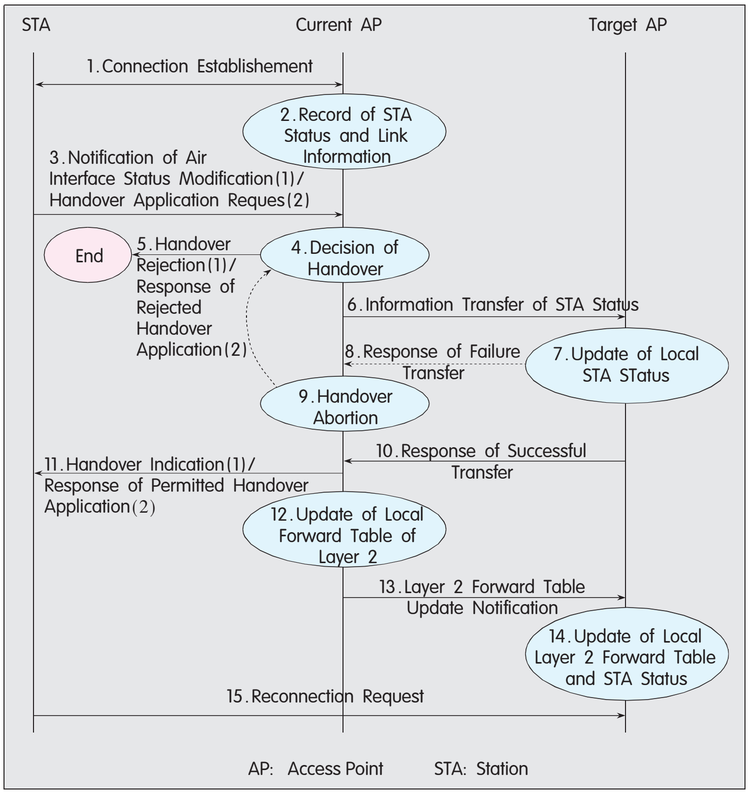
(2) The AP/AC decides whether handover is necessary according to received information of the environment of radio air interface and DS message.

(3) STA information is transferred and the Layer 2 route is updated.

(4) The STA switches to the target AP, and handover is fulfilled.

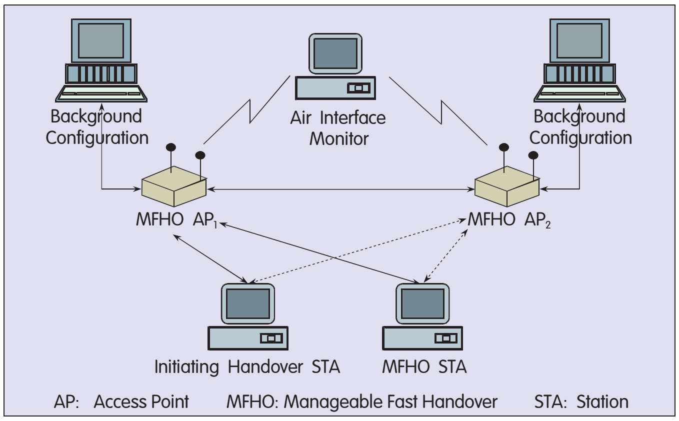
The MFHO can be implemented by two air interface methods, that is, handover indication and handover request. They are different. The former sends the STA related information, including the Basic Service Set Identifier (BSSID), MAC address, authentication status, encryption mode and encryption key, to the AP through the environment of radio air interface (marked by (1) in Figure 2). The latter notifies the AP with STA related information by handover request (marked by (2) in Figure 2). The handover decision may be made at the AP or at the AC of the upper layer with the decision result notified to the AP. After getting the result of the handover decision, the AP replies to the STA with a handover request response or a handover indication notification. The STA then switches to the target AP according to this reply.

The MFHO has several strengths when compared with STA initiating handover. First, the time delay of STA initiating handover is longer, for it is the total time for synchronization, reconnection, and updating the Layer 2 route. However, the time delay of MFHO is just the maximum among the time for synchronization, transferring STA related information, and updating the Layer 2 route. Moreover, MFHO shortens the time delay for authentication during handover by pre-authorization and authorization-dependency technologies, with which mutual authentication between the AP and the AC is fulfilled before handover and the authorization granted by certain an AP can be extended to other reliable APs. Second, the STA initiating handover takes no account of traffic of the target AP, which is more possible to cause frequent handovers among several APs and results in low handover efficiency. The MFHO enables an AP to make handover decision according to its load strategy and distribution of traffic load in the ESS. This greatly improves the handover success rate, and avoids frequent handover. Third, the STA initiating handover has no security guarantee scheme for handover. Though the IAPP supports safe handover based on Remote Authentication Dial In User Service (RADIUS), the handover process with low efficiency is possibly threatened by Denial of Service (DoS) attacks. The MFHO, however, may use the security strategies of wired networks to guarantee mutual authentication and authorization between the AP and AC,



▲Figure 2. Implementation process of an MFHO handover request at AP.

D:\EMAG\2006-02-13/VOL4\DP2.FIT——4PPS/P2



▲Figure 3. MFHO test system.

and ensure the handover security of the STA by handover control at the AP.

1.3 Implementation of MFHO in Access Point

While getting support of STA, the MFHO can be fulfilled at the AP with the following process, which is also shown in Figure 2:

(1) The STA establishes a connection with the current AP.

(2) The current AP stores the messages about the STA connected to it, its own traffic and traffic of the entire wireless network.

(3) The STA sends an air status changing notification or handover request.

(4) The current AP makes handover decision according to the messages of the environment of radio air interface (or handover request) reported by the STA and the messages of DS. According to the air status changing notification or handover request sent by the STA, the AP checks the validity of the target AP. Then, it decides whether to conduct handover and which target AP the STA should be transferred to among several target APs, based on its own traffic and the traffic of the network at that moment. If the current AP does not allow handover, go to (5). If it requests handover, go to (6).

(5) The current AP does nothing, or just sends a refusal response to the handover request. The handover ends.

(6) The current AP copies information about the STA to the target AP via the security channel of DS.

(7) The target AP changes the STA into a handover status. If the transfer of STA information is successful, go to (10); otherwise, go to (8).

(8) The target AP replies to the current AP with a transfer failure response.

(9) The current AP ceases current handover and goes to (5).

(10) The target AP replies to the current AP with a successful transfer response.

(11) After receiving the acknowledgement, the current AP gives the STA a handover indication or a permission response to the handover request to inform it to be switched to the target AP.

(12) The current AP updates the local Layer 2 forward table, modifies the STA route in DS, and then deletes the local STA information.

(13) The current AP broadcasts update of the Layer 2 forward table in DS.

(14) The target AP renews the local Layer 2 forward table and changes the STA into a status of completed handover.

(15) The STA sends reconnection request to access the target AP.

1.4 Test and Performance Analysis

At room temperature, the MFHO test requires the following devices: two ZTE W500A APs that support MFHO, one ZTE W500C wireless network card that supports MFHO, one ordinary ZTE W500C wireless network card, two desktop computers (for background configuration of APs and packet interception of the air interface), and two test laptop computers (supporting installation of wireless network cards). One laptop computer is used for mobile testing, and the other one for monitoring the air interface.

The MFHO test system is demonstrated in Figure 3.

Both MFHO APs are configured with the same ESSID to enable communication terminals to monitor the APs in the same ESS. Moreover, testing software Airopeek is used to monitor air communication. The laptop computers are acting as STAs moving between the two APs to trigger handover, and recording time of the events related to handover.

1.4.1 Handover Success Ratio

The test data shows that AP-based MFHO technologies implemented by handover indication and handover request have successful handover ratios of 100% and 95% respectively (with 50 tests in total). The successful handover ratio is defined as the percentage of successful handover times to the total handover times when the STA uses reconnection requests for handover from the current AP to the target AP. The successful ratio of IAPP-based handover is only 90% (with 50 tests in total). Consequently, the successful ratio of MFHO is a bit higher than that of IAPP-based handover. The reason is that MFHO, during the STA handover process, depends on network information offered by the STA and the AP. The full use of the AP's decision enables the STA to launch reconnection for handover more pertinently and effectively. This is helpful to guarantee the successful ratio.

1.4.2 Performance Analysis

When testing the performance, data at the STA side and in the air are recorded respectively in order to ensure that they are comprehensive and reliable. The result of performance analysis is derived from comparison of the MFHO testing records and the previous testing records of IAPP-based handover technology.

Data at the STA side are classified in three categories:

(1) For the handover-indication-based MFHO process, the time stamps of four events are recorded. They are the time of STA sending the last air interface message, receiving handover indication, sending a reconnection request, and receiving the reconnection request.

(2) For the handover-request-based MFHO process, there are four event time stamps, including the time of STA sending the last handover request, receiving the handover response, sending a reconnection request, and receiving the reconnection response.

(3) For the IAPP-based handover process, three event time

▼Table 1. Statistics of test data at the STA side

Handover-indication-based MFHO	Handover-request-based MFHO	IAPP-based Handover Technology
Time difference between sending the last air interface message and receiving the handover indication is 491.20 ms.	Time difference between sending the last handover request and receiving the handover response is 754.44 ms.	—
Time difference between receiving the handover indication and receiving the reconnection response is 53.16 ms.	Time difference between receiving the handover response and receiving the reconnection response is 56.40 ms.	Time difference between handover decision and receiving the reconnection response is 132.36 ms.
Time difference between sending a reconnection request and receiving the reconnection response is 8.00 ms.	Time difference between sending a reconnection request and receiving the reconnection response is 10.40 ms.	Time difference between sending a reconnection request and receiving the reconnection response is 88.16 ms.

stamps are recorded. They are the time of the STA deciding to conduct handover when it detects a target AP with a stronger signal by background scanning and then breaks the current connection, sending a reconnection request, and receiving the reconnection response.

Three points are concluded according to the test data shown in Table 1.

(1) Compared to handover-request-based MFHO, handover-indication-based MFHO consumes less time for processing before handover, including the time for transferring user information.

(2) Since the transfer of user information is completed before handover, both the handover-indication-based and the handover-request-based MFHO theoretically processes the reconnection request in the same way, and the time for processing is almost equal. However, the time delay for IAPP-based handover is longer, because the target AP needs to get user information from the current AP after handover. This is verified by the test.

(3) The average handover time delay for handover-indication-based and handover-request-based MFHO is respectively 53.16 ms and 56.40 ms, which is greatly superior to 132.36 ms of IAPP-based handover. Furthermore, the MFHO has better handover performance than IAPP-based handover, for MFHO completes most processes including user information transfer before handover and lessens the influence of handover on services. Therefore, multimedia services, such as voice and real-time video services will benefit from MFHO.

2 Conclusions

According to the test results, the MFHO can be implemented at the AP and has shorter handover time delay than IAPP-based handover. It is able to ensure excellent service continuity and high reliability. In MFHO, the user information has been transferred to the target AP before a new connection is initiated and no re-authentication is needed during the reconnection. (The STA does not use any authentication in the test.) This consequently makes MFHO faster than IAPP-based handover. Obviously, in a complex authentication scenario, IAPP-based handover will take longer time for re-authentication during reconnection and MFHO's better handover performance will be more prominent[3-5].

Simplifying the processing at the AP side, reducing processing time as much as possible, optimizing AP handover decision strategy and reviewing the implementation of AC-based MFHO at the AP may further enhance implementation of MFHO at AP.

References

[1] IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification[S]. 1999.
[2] IEEE 802.11f/D3 Recommended Practice for Multi-vendor Access Point Interoperability via an Inter-access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation [S]. 2002.
[3] Heiskala J, Terry J. OFDM无线局域网[M]. 杨晓春,何健吾,等译. 北京：电子工业出版社, 2003.
[4] 佟学俭, 罗涛. OFDM移动通信技术原理与应用[M]. 北京:人民邮电出版社, 2003.
[5] 王文博, 郑侃. 宽带无线通信OFDM技术[M]. 北京:人民邮电出版社, 2003.

Manuscript received: 2006-06-09

Biographies

Gao Yin received her Master's degree from Electronic Engineering School of Xi'an University of Electronic Science and Technology. She works with Mobile Division of ZTE Corporation and is engaged in the study of 3G communication technology.

Li Jie received his Master's degree from Computer Science School of Xi'an University of Electronic Science and Technology. He works with Mobile Division of ZTE Corporation, and is engaged in the study of MAC technology of WLAN.